UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/664,663	09/20/2003	Christopher Reon Gentle	403076-A-01-US (Gentle)	4616

7590 01/11/2007

John C. Moran
Attorney, P.C.
4120 E. 115th Place
Thornton, CO 80233

EXAMINER	
WYSZYNSKI, AUBREY H	
ART UNIT	PAPER NUMBER
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/664,663	GENTLE ET AL.	
	Examiner	Art Unit	
	Aubrey H. Wyszynski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-48 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-2, 5-26, 28-31, 34-43, and 45-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Fauble et al, U.S. Patent Application Publication No. 2003/0159053.

Regarding claims 1 and 42, Fauble discloses a method for protecting data generated by a keyboard/secure keyboard console (fig. 4, #50), comprising the steps of: reading data from a keypad of the keyboard; encrypting the read data (¶[0034], lines 1-17); and transmitting the encrypted data from the keyboard to a computer/second computing device (fig. 4, #44).

Regarding claims 2 and 43, Fauble discloses the method of claim 1 further comprises the steps of receiving the transmitted encrypted data by the computer; and decrypting

the received encrypted data by the computer (¶[0034], lines 17-23).

Regarding claims 5 and 45, Fauble discloses the method of claim 1 wherein the step of encrypting comprises the step of using an encryption seed/public key; and receiving the encryption seed from at least one of the computer or a server (fig. 4, exchange public keys).

Regarding claims 6 and 46, Fauble discloses the method of claim 1 wherein the step of encrypting comprises the step of using an encryption seed; and reading the encryption seed from a device reader connected to the keyboard/smart card reader (fig. 6, #72).

Regarding claim 7, Fauble discloses the method of claim 6 wherein the step of reading the encryption seed comprises the step of enabling the device reader with a personal identification number/unique identification number (¶[0049]).

Regarding claim 8, Fauble discloses the method of claim 1 wherein the step of encrypting comprises the step of receiving a start signal/key depression (¶[0034]).

Regarding claims 9 and 47, Fauble discloses the method of claim 8 wherein the step of receiving the start signal comprises the step of generating the start signal by at least one of a special key on keyboard, multi-actuation of a number of keys on the keypad, the computer, or a server/control button (¶[0029]).

Regarding claim 10, Fauble discloses the method of claim 1 wherein the step of encrypting comprises the step of receiving a stop signal that stops the encryption/key release (¶[0034]).

Regarding claim 11, Fauble discloses the method of claim 10 wherein the step of receiving the stop signal comprises the step of generating the stop signal by at least one of a special key on keyboard, multi-actuation of a number of keys on the keypad, the computer, or a server/control button (¶[0029]).

Regarding claims 12 and 48, Fauble discloses the method of claim 1 further comprises the step of defining operations of the step of encrypting from program information received from at least one of a device reader, the computer, or a server (fig. 7, Bank Server #84, transmits transformation instructions).

Regarding claim 13, Fauble discloses a method for protecting by a computer data generated by a keyboard/secure keyboard console (fig. 7, #50), where the keyboard is connected to the computer/user computing device (fig. 7, #82), comprising the steps of: receiving encrypted data from the keyboard by the computer (¶[0034], lines 10-14); and decrypting the encrypted data (¶[0034], lines 14-23).

Regarding claim 14, Fauble discloses the method of claim 13 wherein the step of

decrypting comprises the step of performing operations of decryption by at least one of a keyboard driver executing on the computer or an application executing on the computer (¶[0058]).

Regarding claim 15, Fauble discloses the method of claim 13 wherein the step of decrypting comprises the step of using a seed/symmetric key (¶[0058]).

Regarding claim 6, Fauble discloses the method of claim 15 wherein the step of using comprises the step of reading the encryption seed from a device reader connected to the computer/smart card reader (fig. 6, #72).

Regarding claim 17, Fauble discloses the method of claim 16 wherein the step of reading the encryption seed comprises the step of enabling the device reader with a personal identification number/unique identification number (¶[0049]).

Regarding claim 18, Fauble discloses the method of claim 13 further comprises the step of generating a start signal to cause the keyboard to start encrypting data/key depression (¶[0034]).

Regarding claim 19, Fauble discloses the method of claim 13 further comprises the step of generating a stop signal to cause the keyboard to stop encrypting data/key release (¶[0034]).

Regarding claim 20, Fauble discloses the method of claim 13 further comprises the step of transmitting program information to the keyboard to define encryption operations (fig. 7, Bank Server #84, transmits transformation instructions).

Regarding claim 21, Fauble discloses a method for protecting by a server data generated by a keyboard/secure keyboard console (fig. 7, #50), where the keyboard is connected to the server/bank server (fig. 7, #84) via a network/global network, and a computer/user computing device (fig. 7, #82), comprising the steps of: receiving encrypted data from the keyboard by the server; and decrypting the encrypted data (¶[0034]).

Regarding claim 22, Fauble discloses the method of claim 21 wherein the step of decrypting comprises the step of performing operations of decryption an application executing on the server (¶[0058]).

Regarding claim 23, Fauble discloses the method of claim 21 further comprises the step of generating a start signal to cause the keyboard to start encrypting data/key depression (¶[0034]).

Regarding claim 24, Fauble discloses the method of claim 21 further comprises the step of generating a stop signal to cause the keyboard to stop encrypting data/key release

(¶[0034]).

Regarding claim 25, Fauble discloses the method of claim 21 further comprises the step of transmitting program information to the keyboard to define encryption operations (fig. 7, encryption key and transformation instruction).

Regarding claim 26, Fauble discloses a keyboard/secure keyboard console (fig. 7, #50), for encrypting data before transmission to a computer/user computing device (fig. 7, #82) connected to the keyboard via a link/keyboard cable, comprising: an interface connected to the link/user computing device; a memory (fig. 7, #54, 56, 58); a keypad for generating the data; a processor/keyboard processor (fig. 7, #60), for encrypting the generated data by execution of an encryption routine stored in the memory; and transmitting the encrypted data to the computer via the interface and link (¶[0034]).

Regarding claim 28, Fauble discloses the keyboard of claim 26 comprises a device reader for reading a device to obtain a seed for the encryption routine (fig. 6, #72).

Regarding claim 29, Fauble discloses the keyboard of claim 26 comprises the processor executing a control routine to receive the encryption routine from at least one of the computer or a server and to store the received encryption routine in the memory/user computing device processor (fig. 7, #90).

Regarding claim 30, Fauble discloses the keyboard of claim 26 comprises a special key which when actuated causes the processor to at least start executing the encryption routine or stop executing the encryption routine/control button (¶[0029] & [0034]).

Regarding claim 31, Fauble discloses a processor-readable medium for protecting data generated by a keyboard/secure keyboard console (fig. 7, #50), comprising processor-executable instructions configured for: reading data from a keypad of the keyboard; encrypting the read data; and transmitting the encrypted data from the keyboard to a computer (¶[0034], lines 1-17).

As per claims 34-41, this is a processor-readable medium version of the claimed method discussed above in claims 5-12 wherein all claimed limitations have also been addressed and/or cited as set forth above.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3-4, 27, 32-33 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fauble as applied to claims 1, 26, and 31 above, and further in view of Arling et al., U.S. Patent Application Publication No. 2004/0117632.

Regarding claim 3, Fauble discloses the method of claim 1. Fauble lacks or does not expressly disclose wherein the step of transmitting comprises the step of using a wireless link over which the encrypted data is transmitted. However, Arling discloses wherein the step of transmitting comprises the step of using a wireless link over which the encrypted data is transmitted (¶[0023]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Fauble with the device of Arling to wirelessly transmit the encrypted data in order to utilize wireless transmission, as taught by Arling (¶[0023]).

Regarding claims 4 and 44, Fauble discloses the method of claim 1. Fauble lacks or does not expressly disclose wherein the step of encrypting comprises the step of using an encryption seed; and entering the encryption seed via the keypad. However, Arling discloses wherein the step of encrypting comprises the step of using an encryption seed; and entering the encryption seed via the keypad (¶[0040]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Fauble with the device of Arling to allow the user to enter the encryption seed in order to ensure the correct proper encryption key value, as taught by Arling (¶[0040]).

Regarding claim 27, Fauble discloses the keyboard of claim 26. Fauble lacks or does not expressly disclose wherein the step of transmitting comprises the step of using a

wireless link over which the encrypted data is transmitted. However, Arling discloses wherein the step of transmitting comprises the step of using a wireless link over which the encrypted data is transmitted (¶[0023]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Fauble with the device of Arling to wirelessly transmit the encrypted data in order to utilize wireless transmission, as taught by Arling (¶[0023]).

Regarding claim 32, Fauble discloses the processor-readable medium of claim 31. Fauble lacks or does not expressly disclose wherein the step of transmitting comprises the step of using a wireless link over which the encrypted data is transmitted. However, Arling discloses wherein the step of transmitting comprises the step of using a wireless link over which the encrypted data is transmitted (¶[0023]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Fauble with the device of Arling to wirelessly transmit the encrypted data in order to utilize wireless transmission, as taught by Arling (¶[0023]).

Regarding claim 33, Fauble discloses the processor-readable medium of claim 31. Fauble lacks or does not expressly disclose wherein the step of encrypting comprises the step of using an encryption seed; and entering the encryption seed via the keypad. However, Arling discloses wherein the step of encrypting comprises the step of using an encryption seed; and entering the encryption seed via the keypad (¶[0040]). It would have been obvious to one of ordinary skill in the art at the time the invention was made

to modify the device of Fauble with the device of Arling to allow the user to enter the encryption seed in order to ensure the correct proper encryption key value, as taught by Arling (¶[0040]).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Wyszynski whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AHW

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100